Future Banking and Financial Attacks

Konstantinos Karagiannis

Director, Ethical Hacking, BT Advise Assure

Global Services

Bringing it all together

89,000 employees globally

= 1,000

Across more than **170** countries

Providing high quality telecommunications services since **1846**

Revenues of more than **£7bn** in 2012/13

We serve around **7,000** corporate & public sector customers

Helping **Unilever** grow its business, while reducing its environmental footprint

"Few companies can offer such world-class, global, innovative and sustainable solutions to help us achieve our ambitious vision."

Maximising supply chain performance for **Rodenstock**

"The BT network is an essential component in the realisation of our corporate IT strategy. It helps streamline the supply chain, enables cost effective manufacture, and supports growth into emerging markets, especially in Asia."

We have relationships with 25 universities globally, including Cambridge, MIT and Tsinghua

We carried every call, byte of data, image and sports report for the London 2012 Olympic and Paralympic Games.

Helping **Fiat** race ahead with global network outsourcing

"The BT outsource solution has allowed FIAT Group companies to focus on core business and deliver efficiency gains and productivity improvement without needing to worry about the IT environment."

Managing a global infrastructure across 119 countries for **British American Tobacco**

"We were impressed with BT's extensive global network, their desire and ability to improve the services continuously through innovation."

BT has invested more than £3.8bn in R&D over the last five years

BT has a total worldwide portfolio of more than 4,300 patents and applications

Empowering a financial services transformation in a changing market for **Standard Life**

"Working very closely with BT, we achieved the migration in an incredible seven months. Our experience is that normal transformation programmes of this type would take about three-and-a-half years. That's a six-fold improvement."

Experts say

- **A Leader**
  Gartner Magic Quadrant for Global Network Service Providers, March 2013*
- **Outstanding overall product viability**
  Gartner's Critical Capabilities for Pan-European Network Services March 2013*
- **A Leader**
  Gartner Magic Quadrant for Communications Outsourcing and Professional Services December 2012*
- **Highly ranked**
  Dow Jones Sustainability World Index (achieving 92% in 2012)

94% of the FTSE100 companies

74% of the Fortune 500 companies

100% of Interbrand's top 50 annual ranking of the world's most valuable brands

*Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Agenda/topics covered

- Threat overview
- Advanced User Enumeration and DDoS
- Trading Turret and Timing Attacks
- Internal and External User Attacks
- A Future Sea Change?

About Me and Futurism

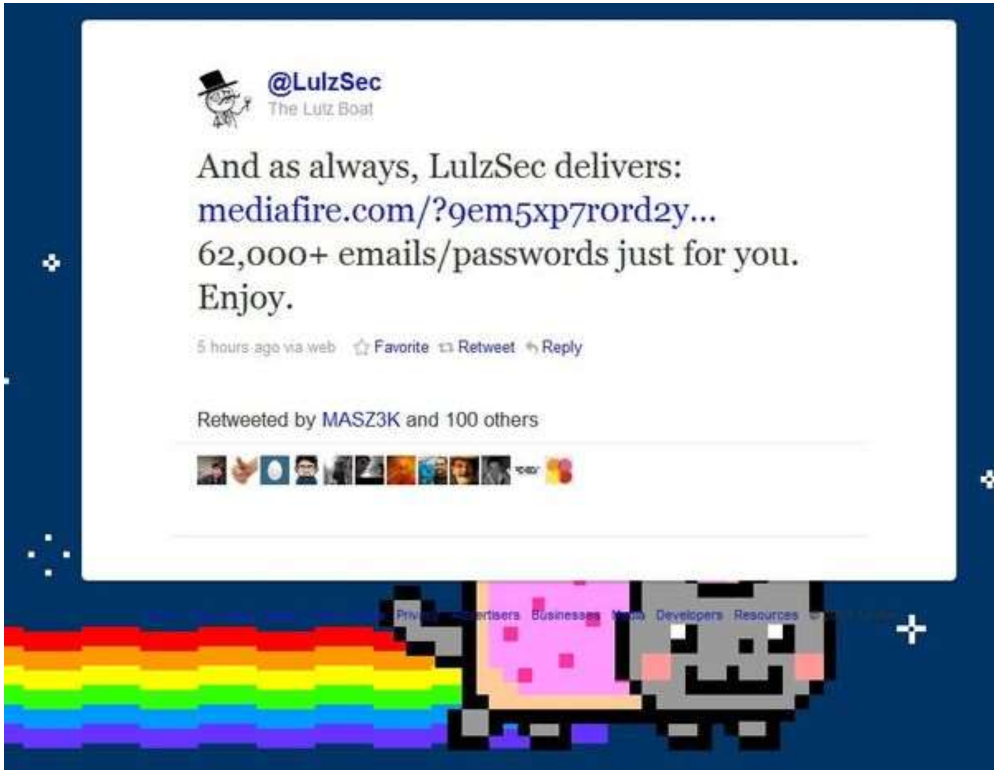
- Half my time breaking into banks, half talking about what we do and aligning
- Started as a Physics major, always looking ahead
- The majority of this talk looks ahead to attacks that are likely to happen soon
- One attack I pitched/predicted for this talk happen in interim

Not just for the lulz these days

- Dark days ahead as cyber attackers get more daring
- Hacktivism got into full swing 5 years ago with agendas:
  - Anonymous and Botnets as payback
  - LulzSec and new antisec movement
- APTs rose as devastating threat—seemingly every company had one
- Financial institutions are the ultimate targets for today and tomorrow

Advanced user enumeration

- Full credentials always a major score (bonus if used at multiple sites)
- SQLi led to most of the LulzSec data dumps—sad, as attack's 13 years old!
- Let's consider the value of just a user ID



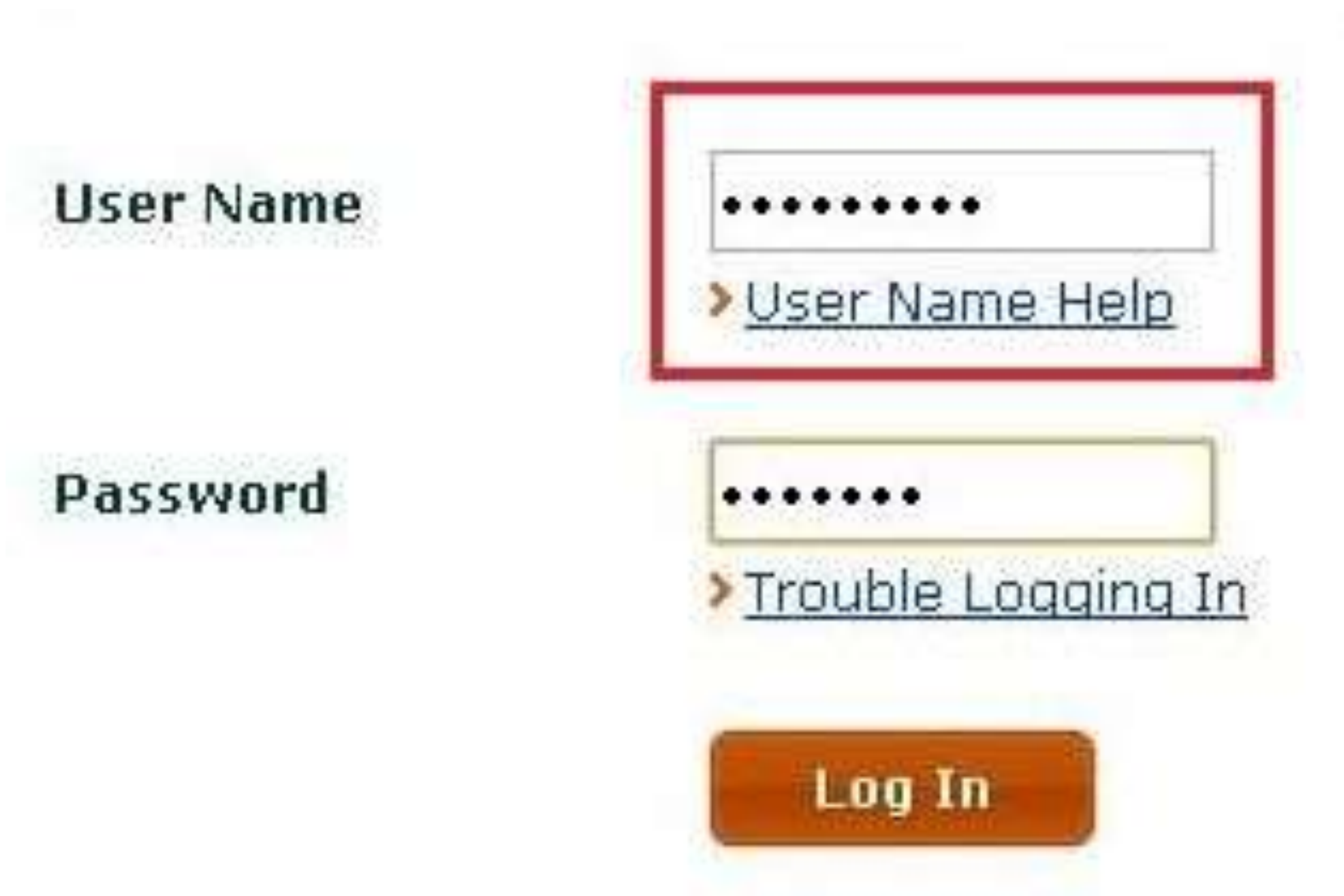
@LulzSec
The Lulz Boat

And as always, LulzSec delivers: mediafire.com/?9em5xp7r0rd2y... 62,000+ emails/passwords just for you. Enjoy.

5 hours ago via web ☆ Favorite ⇄ Retweet ↰ Reply

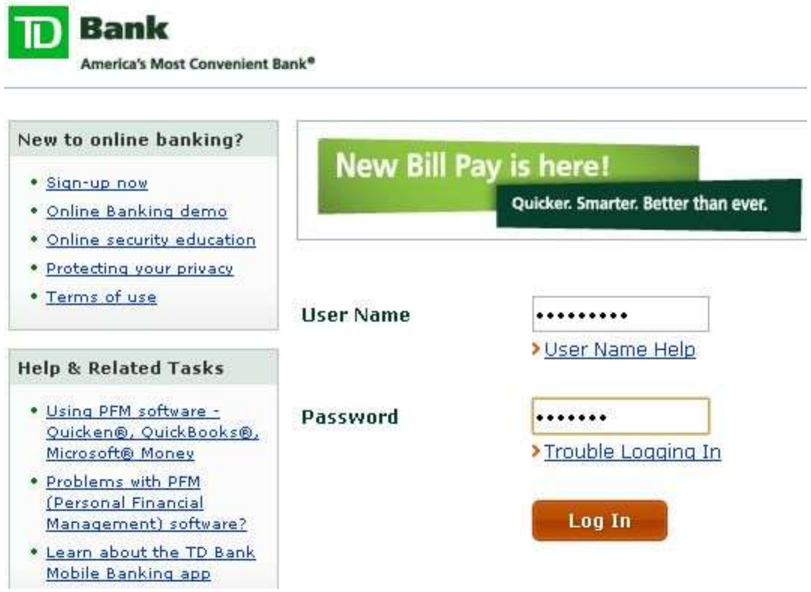
Retweeted by MASZ3K and 100 others

How Often Do You See This?



Don’t Just Give it Away

- Kudos to TD Bank
- Masking a user ID is important—prevent autocomplete too!
- User IDs without passwords are valuable in financial institutions
- Shoulder surf or autocomplete to
  - Guess a password (not likely)
  - Lock an account and disrupt activity (more likely)
- What if you can get ALL user IDs?



TD Bank
America's Most Convenient Bank®

New to online banking?

- Sign-up now
- Online Banking demo
- Online security education
- Protecting your privacy
- Terms of use

Help & Related Tasks

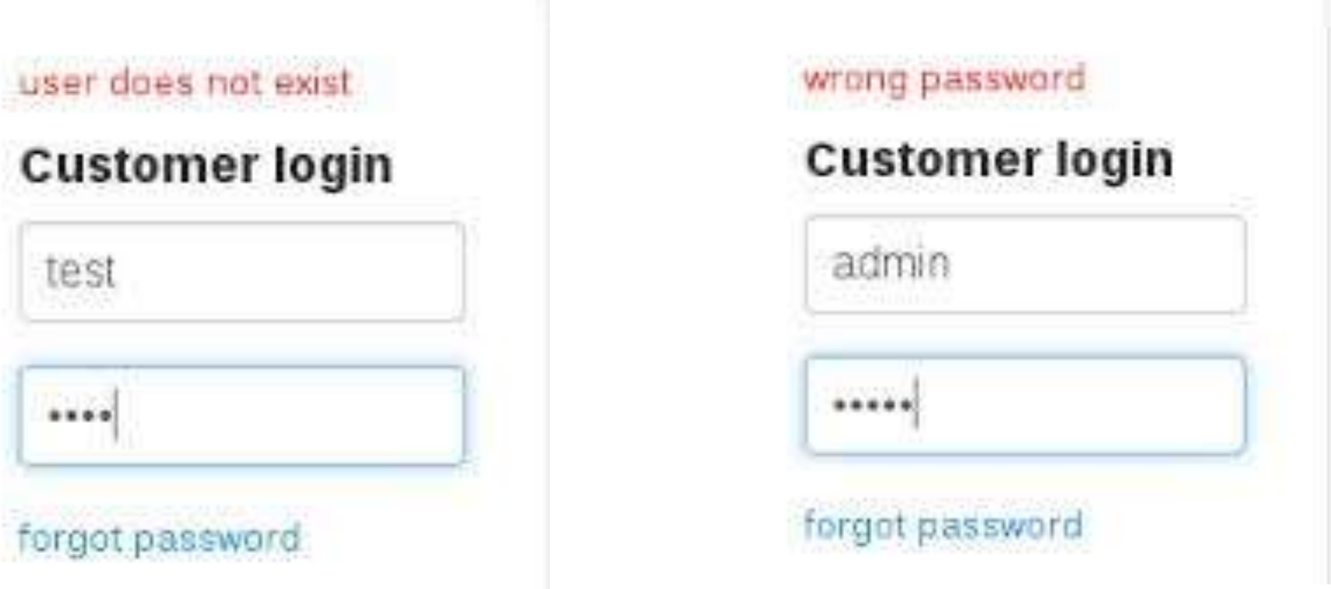
- Using PFM software - Quicken®, QuickBooks®, Microsoft® Money
- Problems with PFM (Personal Financial Management) software?
- Learn about the TD Bank Mobile Banking app

New Bill Pay is here!
Quicker. Smarter. Better than ever.

User Name: •••••••••
› User Name Help

Password: •••••••
› Trouble Logging In

More often we see response pairs like these…



user does not exist

Customer login

test

••••

forgot password

wrong password

Customer login

admin

•••••

forgot password

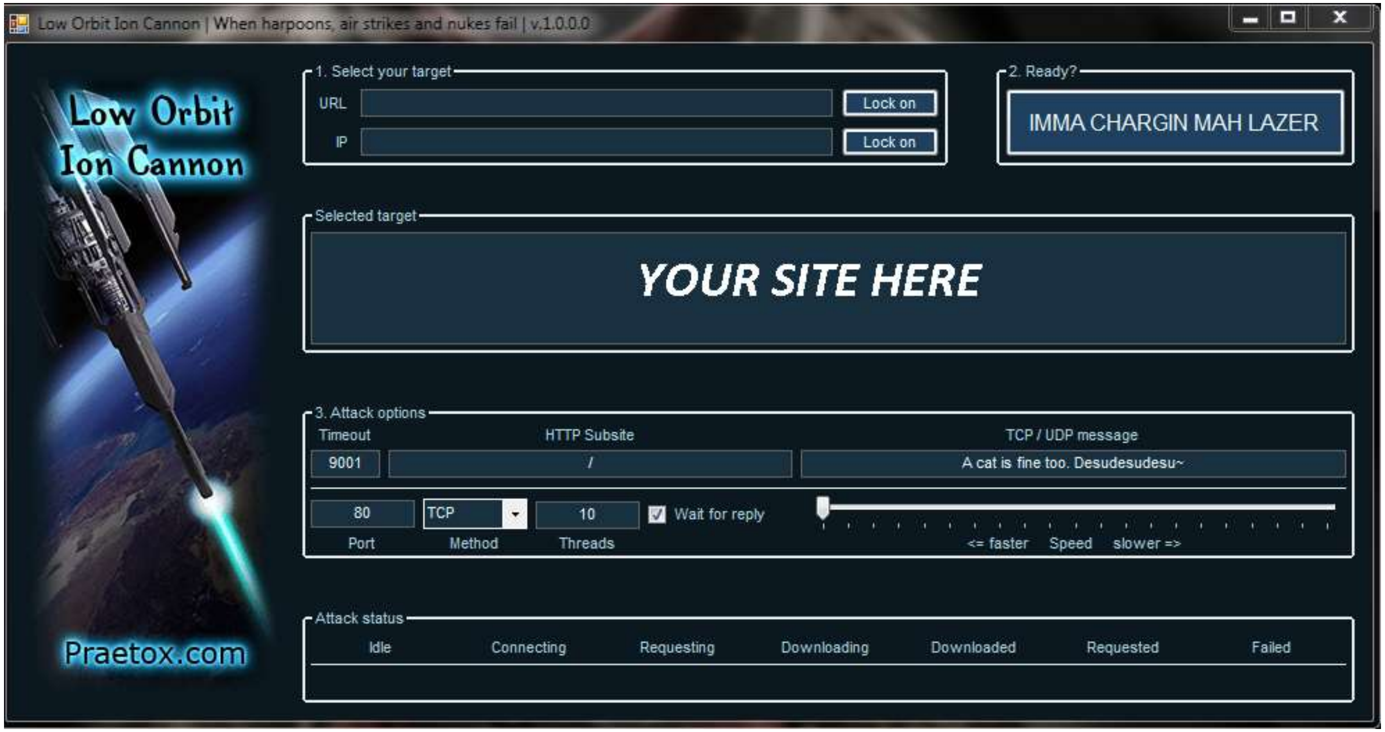
- Response difference makes it trivial to grab all users
- An army of machines can be assigned harvesting
- Same army can be used to do some damage with results

Traditional DDoS

- Sending massive amounts of traffic to a site, knocking it out for a period of time
- Works on network or app layer
- Brutish, old news? Ask Paypal, Scientology and other victims
- A favorite tactic of Anonymous and other groups
- Can have impact in lost transactions—damage to reputation

How volunteers thought DDoS works

- Anonymous would tell “troops” in 4Chan B group to use LOIC against targets
- LOIC sends heavy traffic to a target (usually traceable—arrests followed)
- Attacking Paypal with LOIC failed—Anonymous needed a secret weapon



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fail | v.1.0.0.0

1. Select your target

URL

IP

Selected target

3. Attack options

Timeout: 9001

HTTP Subsite: /

TCP / UDP message: A cat is fine too. Desudesudesu~

Port: 80

Method: TCP

Threads: 10

☑ Wait for reply

Attack status

How DDoS really worked

- In private IRC channels, Anonymous wielded real strength in numbers
- Members with botnets would point up to 50,000 hacked machines each
- These botnets are often rented out by the hour or day

Imagine…

- A botnet that harvests all users then performs a simultaneous attack
- One vector is mass lockout
  - Cost to helpdesks
  - Lost productivity/transactions
  - Move to a competitor’s system
  - Use lockout to hide another attack
- Another is simultaneous brute force
  - A few of 50,000 users may have a simple password
  - Enough users makes for even simple token function cracking

Trading Turret and Timing Attacks

- Let me tell you a story…
- August 22, 2013 – NASDAQ
- Arca tried to connect more than a whopping 20 times to Nasdaq price system
- Sent standard zero-dollar quotes to ensure no stale trades sent
- SIP had to flip to a backup server to handle “flood”—backup system had an unknown flaw
- Caused a form of DoS for 3 hours
- Not hackers … but couldn’t it one day be?

In Trading, Even Milliseconds Count Big

- Accidental DoS didn’t cause depression-like runs on banks
- In high frequency trading, losing millisecond advantages could cost millions per second
- These systems are being targeted now
- CME Group disclosed a breach in July of its ClearPort platform

Trading platforms

- Trading platforms becoming webified
- Plagued by weak passwords, long timeouts, and general bugs
- Was going to speculate about effects of layer 7 DDoS on these newer, “convenient” platforms
- Last month, it actually happened to an Incapsula customer
  - 180,000 bots
  - 150 hours
  - 700 million hits/day
  - Headless browser—Phantom JS toolkit—for 861 different traffic variants

Trading turrets

- DDoS already used to gain competitive edge in the web
- Turret and platform combos appear similarly vulnerable—web interfaces especially
- Trading turrets actually juggle tech from phone lines to VM systems:
  - Difficult to gauge trust levels—a hypervisor hack to feed false data?
  - Access to adjacent network could be disastrous
  - Electronic interference devices being deployed outside building?

Trading systems need further testing for the future

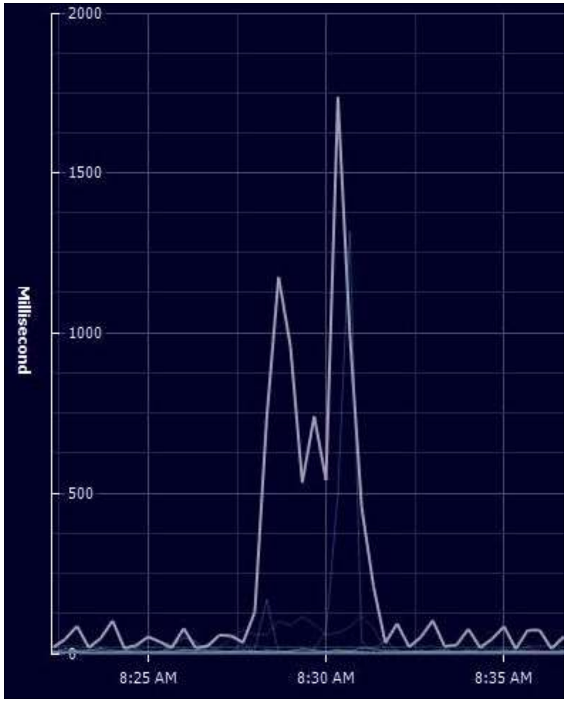
- Financial system hacking events hope to spot unpredictable
  - British Bank Cyber War Games
  - NY Quantum Dawn 2
- These hackfests are designed to simulate DDoS and other attacks
- We’re finding the balance in financial systems is beyond delicate

It’s horrifying what’s being found…

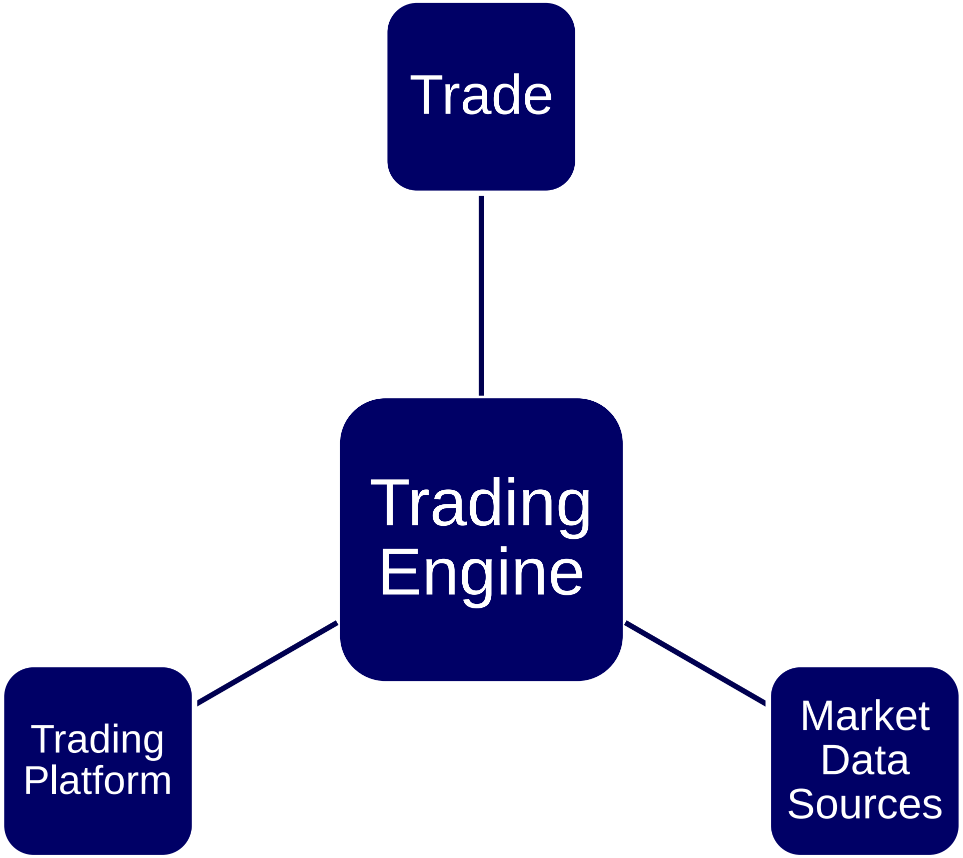
- Low tolerance for errors makes trading systems attractive targets
- High-frequency trading—where milliseconds equal millions lost
- Developers are not security guys
- Servers kept close to cut down even on light speed’s impact
- Many use minimal hardening to achieve maximum performance
- Custom interfaces rather than firewalls and ACLs?!
- Highly susceptible to disgruntled employee type attacks

Timing attacks can target…

- Network interface already a delay for packetizing
- Network processing delays at firewalls, gateways, security devices (if any)
- Signal propagation delay by cable length
- Router and switch delay
- Queuing delay from packets trying to leave hardware

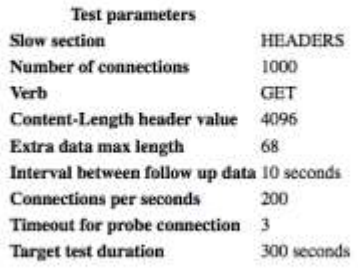


Key stress points

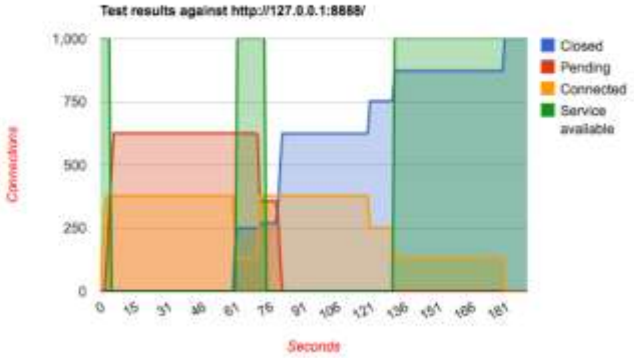


Components of trading systems need DDoS protection

- DDoS by massive network traffic hard to fight
  - Requires impressive load balancing and monitoring
  - BT has Managed Security services and Assure Denial of Service Mitigation
  - Partner Prolexic protected Henyep Capital Markets platform attack
- DDoS by app flaws (such as slow HTTP requests that hang servers) easier to test for
  - slowloris
  - siege
  - slowhttptest
- Layered defenses needed



Test parameters	
Slow section	HEADERS
Number of connections	1000
Verb	GET
Content-Length header value	4096
Extra data max length	68
Interval between follow up data	10 seconds
Connections per seconds	200
Timeout for probe connection	3
Target test duration	300 seconds



Test results against http://127.0.0.1:8888/

Imagine

- A 13-year-old exploit taking down an entire trading system through a web interface
- Interference/jamming techniques knocking a system’s transmissions out of sync from a parking lot
- Attackers repeating different vectors for hire to get their “employer” an edge of billions of dollars

APTs—Seems everyone has them?

- We've all heard of them, but a high level of their attack stages is helpful:
  - System infection
  - Malware download
  - Callbacks
  - Data exfiltration
  - Lateral movement

The New York Times

HACKED!

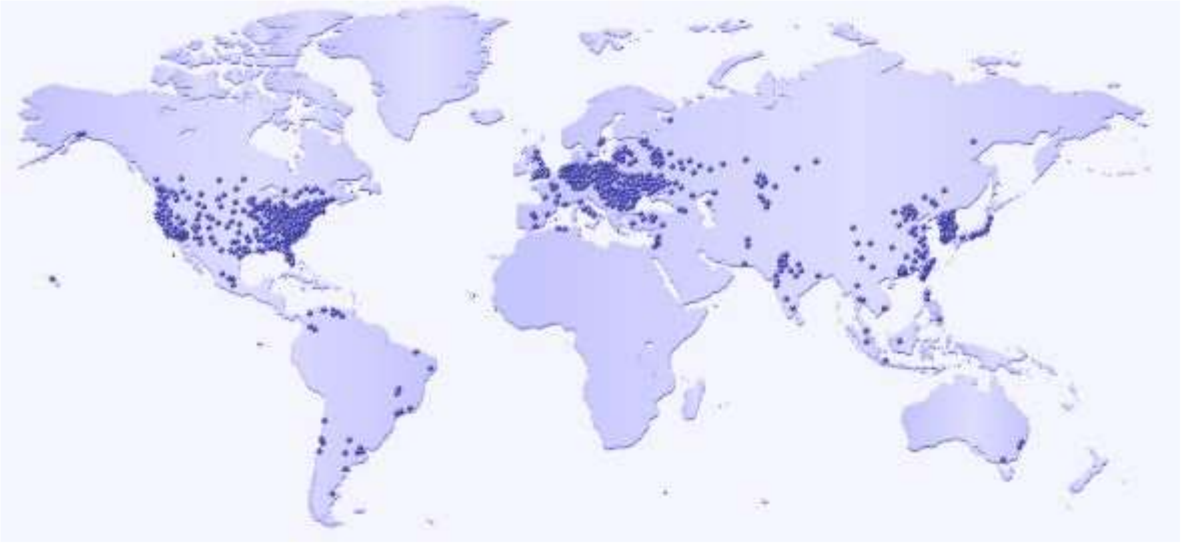
<insert company name here>

Internal User Attacks and APTs

- Attackers only beginning to exploit having an internal foothold
- Future APTs will make possible massive, simultaneous attacks on end user accounts and funds
- Rather than noisy exfiltration of mass amounts of data, future APTs will target specific privileged users
- An intelligent ghost in the machine

Internal User Attacks—Intelligence

- Already seeing better APT exfiltration
- Encoded information in JPGs or in social media posts
- APTs to only phone home with privileged user data for multi-prong attack
- Currently 80 days or more until discovery, up to 200 for cleanup!

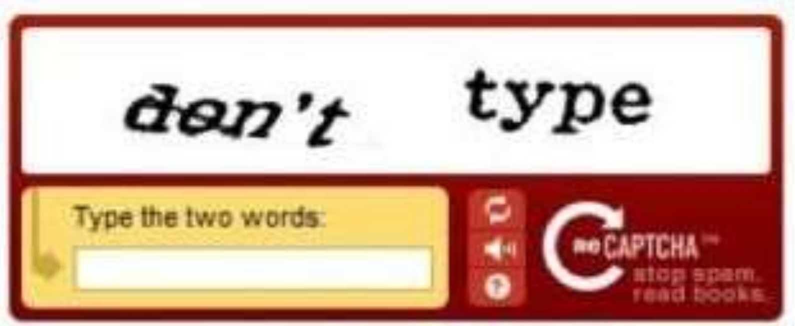


External User Attacks and MitE

- New malware to allow for fraudulent actions and theft to occur on the victim’s machine.
- Forget sniffing passwords—focus on transfers occurring from trusted sessions and IP addresses
- Man-in-the-Endpoint (MitE) attacks could bypass even multi-factor authentication
- MitE responsible for a multimillion dollar cyber theft 3 years ago—expect it to get better at finding victims

Coding against MitE

- Sensitive transactions need CSRF-like protection to ensure humans at helm
- Never allow important transaction to occur with simple GET—multi-step
- Re-authenticate for major transactions
- Technology like CAPTCHA
- Short timeouts: < 20 minutes
- Constantly changing, non-predictable session IDs or tokens appended to each transaction



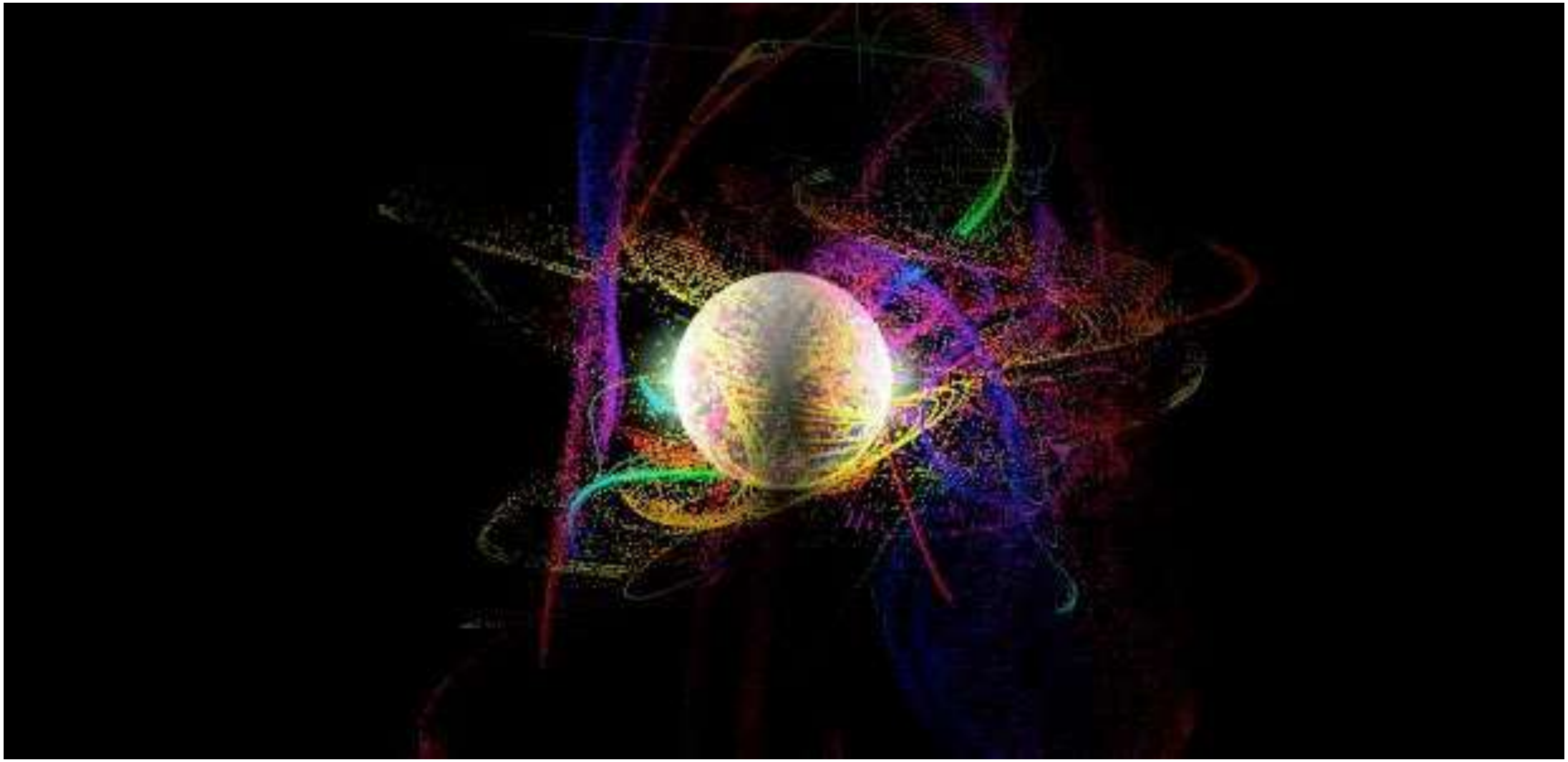
Preventing APTs

- Could “dated” honeypots be the answer to our APT problem?
- They certainly give great look at what’s going on in a network
- Set up dummy accounts and servers we know shouldn’t have activity, catch APTs in action
- Bad traffic should be darknetted
- Companies like Fire Eye are doing something along these lines

Imagine

- APTs so advanced that they coexist with one another to accomplish parallel devastation
- Malware that can take an entire corporation hostage
- End users losing subtle amounts of money for years without knowing it

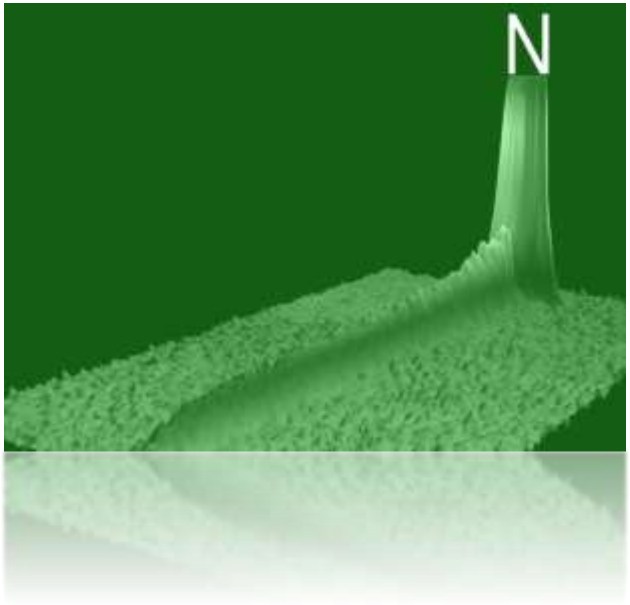
And now for a seriously futuristic, future threat…



Who will get a Quantum Computer First?

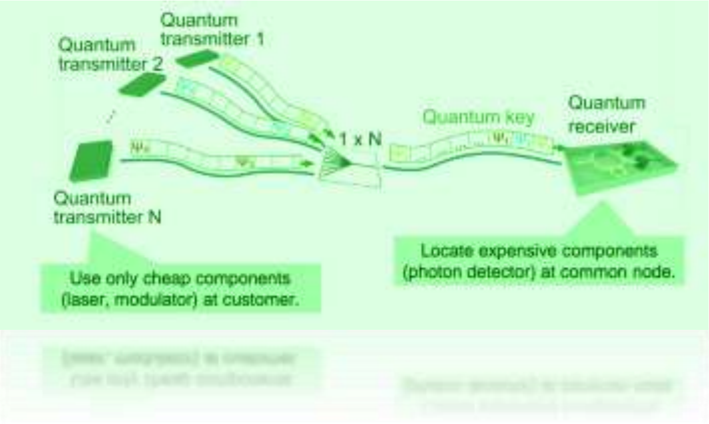
- Particles can be kept in superposition—allows for qubits (zero, one, or both)
- Qubits in a quantum computer will be able to try all problem solutions at once
- Could find large factors of numbers in seconds, shattering RSA PK crypto—Shor’s Algorithm
- Faster database searches with Grover’s Algorithm (bye DES)
- Developments in this field almost weekly—last week a qubit was kept for 39 minutes in a usable state
- Quantum computers within this decade

$$\alpha|0\rangle + \beta|1\rangle$$



Staying Relevant—Encryption

- The following haven't fallen on chalkboards:
  - Lattice based (NTRU)
  - Code based (McEliece's Goppa code)
  - Hash based (Merkle's hash tree)
  - Multivariate quadratic equations (HFE^{V-})
- Toshiba working on quantum encryption:
  - Polarized photons carry encryption key via fiber optic cable
  - Tampering with photons changes packets
  - Detector can count 1 billion photons/sec
- Can support 64 users, unlike recent, expensive 2-user setups


Quantum transmitter 1
Quantum transmitter 2
Quantum transmitter N
1 x N
Quantum key
Quantum receiver
Use only cheap components (laser, modulator) at customer.
Locate expensive components (photon detector) at common node.

Questions?

Thank you

konstantinos.karagiannis@bt.com

http://www.bt.com/security

http://www.btsecurethinking.com